REMARKS

The Office Action mailed May 28, 2008, was received and its contents carefully reviewed. Claims 1-79 were originally pending prior to the Office Action of May 28, 2008. In the above amendments, Applicants amended independent claims 1 and 37 to highlight additional features of the invention and to provide additional context to the claims. The features are disclosed at least in paragraphs [0022, 0053, 0059-0062, 0066, 0067, 0088, 0092, and 0108] and throughout the Specification and Figures. Applicants respectfully submit that no new matter was introduced by these amendments. As now recited, claims 1-79 remain pending and are believed to be in condition for allowance. Applicants respectfully request reconsideration of this application in light of the above amendments and the following remarks.

A. Allowable Subject Matter

Applicants acknowledge and thank Examiner Dada for the indication that claims 24, 25, 35, 60, 61, and 71 recite allowable subject matter and were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

B. Claim Rejections Under 35 U.S.C. § 112, first paragraph

Claims 77 and 79 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement as indicated on page 3 of the final Office Action mailed May 28, 2008. Applicants respectfully request reconsideration and withdrawal of this rejection because the specification properly discloses a system and a method where the security module is installed on a client computer at a different time than the standard application program.

The present invention relates to a system and method for controlling use of digital content that has usage rights associated with the content. The system for distributing digital documents with associated usage rights includes a server having at

least one digital document stored on it, a client computer with a standard application program including a rendering engine capable of being accessed to render content, a communications network coupled to the client and the server, and a security module adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine. See paragraph [0022] of the present specification as well as claims 1, 37, 77, and 79.

As described in the original specification, a preferred embodiment of the present invention utilizes a standard rendering engine of an application program, such as a browser, a word processor, or any other application or display program. The preferred embodiment achieves this by interfacing with the application and standing between the application and the document to control access to the document. Accordingly, a separate proprietary rendering engine for each document format is not required. Further, any data format supported by the application will be supposed by the invention without modification. The preferred embodiment permits digital rights management (DRM) systems to be adapted to standards, such as TCP/IP and the use of browsers to render HTML. Further, the preferred embodiment of the present invention facilitates various functions that permit DRM to be applied to systems in a manner that is transparent to the user. See paragraph [0063] of the present specification.

For example, "[A] client computer 230 initially does not have all required components of security module 237 installed therein." See paragraph [0064]. Client computer 230 makes a request of distributor server 220 for one or more documents 222 in step 502 of the method described in paragraph [0064] of the present specification. "Distributor server 220 analyzes the request and, based on a lack of signature information within the request (indicating that components of security module 237 are not loaded in client computer 230), sends a response to client computer 230 to load the requisite components of security module 237 in step 504." See paragraph [0064] (emphasis added). As noted throughout the specification, security module 237 functions to enforce usage rights in client computer 230.

When the client computer 230 receives the response to load the components of security module 237, it also executes a software component that includes information about where to get the components of security module 237 that are not present. See step 506 of Figure 5 and the corresponding description in paragraph [0065] of the present application. In step 508, "Client computer 230 receives and installs the components of security module 237." See paragraph [0065] of the present specification.

A standard application program may be an Internet Web Browser, as indicated in the Field of Invention of the specification, whereby, "The invention relates to distribution of digital content, and more particularly, to a method and apparatus for facilitating distribution of protected documents displayed with the rendering engine of a standard application program, such as an Internet Web Browser." See paragraph [0002] of the present specification (emphasis added). See also paragraph [0022]. Further, "[C]lient 230 includes browser 232 as a standard application program having a rendering engine." The phrase "standard application program", as used in the present application, "... refers to any application program designed to accomplish a task, such as document creation, viewing and editing, and having a rendering engine. Examples of standard application programs include word processors, Web browsers, editors, viewers, spreadsheet programs, database programs, and the like." See paragraph [0049].

As described in paragraphs [0063-0065] of the present specification, the client computer first uses a standard application program to make a request of distributor server 220 for one or more documents. Distributor server checks the requests and finds that client computer does not have the requisite security module. Distributor server responds by sending client computer an indication that client computer needs to load the requisite components of security module 237. Client computer then installs the components of security module 237. That is, client computer first uses a standard application program to make a request of distributor server 220 for one or more documents 222 and later, at a different time, installs the security module. As such, the security module is installed on the client computer at a different time than the standard

application program. Therefore, there is ample support in the present specification to support claim 77, which recites a system wherein the security module is installed on the client computer at a different time than the standard application program as well as claim 79, which recites a method where the security module is installed on the client computer at a different time than the standard application program.

As such, Applicants respectfully submit that the claimed subject matter is properly described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Applicants respectfully request reconsideration and withdrawal of the rejection of claims 77 and 79 under 35 U.S.C. § 112, first paragraph.

C. Claim Rejections under 35 U.S.C. § 103

Claims 1-23, 26-34, 36-59, 62-70, 72, and 76-79 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Peinado et al. U.S. Patent Number 6,816,596 ("the Peinado patent") in view of Rabin et al. U.S. Patent Number 6,697,948 ("the Rabin patent") as indicated beginning on page 3 of the May 28, 2008, final Office Action. In view of the amendments above and the comments below, Applicants respectfully request reconsideration and withdrawal of this rejection because the combination of the Peinado patent and the Rabin patent fails to disclose or suggest all the elements recited in the pending claims and fails to make the claimed invention unpatentable as obvious under 35 U.S.C. § 103(a).

The present invention is generally directed to systems and methods for the secure distribution and consumption of electronic documents using a standard rendering engine. The present invention is used to control the use of digital content that has usage rights associated with the content. The system for distributing digital documents with associated usage rights includes a server having a digital document stored on it, a client computer with a standard application program including a rendering engine to be accessed to render content, a communications network coupled

to the client and the server, and a security module adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine. See paragraph [0022] of the present specification.

1. The Combination of the Peinado Patent and the Rabin Patent Fails to Disclose or Suggest All the Features Recited in Amended Independent Claim 1.

Independent claim 1 recites a system for controlling use of digital content that has usage rights associated with the content. The system for controlling content includes a server with digital content stored on the server. See, for example, Figs. 2 and 3, and the discussions that follow in at least paragraphs [0022, 0049-0052] and throughout the specification discussing distributor server 220. The system also includes a client computer with a standard application program including a rendering engine capable of being accessed to render content. See, for example, Figs. 2, 3, 7, 8, 10, and 11, and the discussions that follow in at least paragraphs [0022, 0049, 0051-0055, 0057, 0058, 0064-0072, 0078-0081, 0086-0088] and throughout the specification discussing client computer 230.

The system of claim 1 also includes a communications network coupled to the client and the server, and a client side security module that is separate from the rendering engine. See, for example, Figs. 2 and 10, and the discussions that follow in at least paragraphs [0003, 0022, 0049, 0052, 0057, 0078, 0113, 0114] and throughout the specification discussing communications network 300. See also, Figs. 2, 5, 6, 11, 13 and the discussions that follow in at least paragraphs [0022, 0049, 0051-0062, 0064-0067, 0078-082, 0086-0092, 0098-0105, 0108, 0111, 0114] and throughout the specification discussing security module 237. The client side security module is downloaded and is included in the client computer. The client side security module is adapted to attach to the standard application program for enforcing security conditions for accessing the rendering engine. See also, Figs. 2, 5, 6, 11, 13 and the discussions that follow in at least paragraphs [0002, 0005, 0015, 0019, 0022, 0049, 0053, 0054,

0059, 0063, 0074] and throughout the specification discussing Web browser 232 as a standard application program.

Further, amended independent claim 1 recites that the security module determines if the requested digital content is protected content, and if the requested digital content is protected content, the security module intercepts a request to the rendering engine to render the protected digital content. Amended independent claim 1 further recites that if the security module determines that the requested digital content is protected content, the security module determines whether to allow a user to perform a requested function on the protected digital content based upon the usage rights associated with the protected digital content. The security module then responds to the request to perform the requested function on the protected digital content based on the usage rights associated with the protected digital content. However, if the security module determines that the requested digital content is not protected content, the security module disengages from the rendering engine to preserve resources of the client computer. See Fig. 4, step 410 (step E) and paragraphs [0059-0061] for intercepting the request. See Figs. 2 and 4, regarding security module 237, UI module 234, and connection module 236 and paragraphs [0053-0061] for determining if the requested digital content is protected content and granting or denying the requested function based on the usage rights associated with the digital content.

(a) The Peinado Patent Fails to Disclose or Suggest the Security Module with the Features Recited in Claim 1.

The Peinado patent does not disclose or suggest a security module that selectively intercepts a request to the rendering engine to render the digital content based upon the usage rights associated with the digital content. Instead, the Peinado patent discusses a black box that performs decryption and encryption functions for the DRM system of the Peinado patent. See col. 3, lines 26-28 of the Peinado patent. See also col. 15, lines 52-63. The black box of the Peinado patent includes a public/private key pair, a version number and a unique signature, all as provided by an

approved certifying authority. See col. 3, lines 28-31 and col. 15, lines 52-63. The black box of the Peinado patent works in conjunction with a license evaluator to decrypt and encrypt information as part of a license evaluation function. See col. 15, lines 55-57. While the Peinado patent employs a black box decryption/encryption module as part of a digital rights management system, there is no disclosure or suggestion of a security module that selectively intercepts a request to a rendering engine to render digital content if the requested digital content is protected content. These features are not disclosed or suggested in the cited Peinado patent, nor is there any suggestion or motivation to modify the system of the Peinado patent to produce Applicants' system recited in amended independent claim 1 of the present application.

In the final Office Action mailed May 28, 2008, the Examiner concedes that the Peinado patent does not disclose a system where a security module [selectively] intercepts a request to the rendering engine to render the digital content. See the last full paragraph on page 4 of the Office Action mailed May 28, 2008. The Examiner relies upon the Rabin patent to remedy the shortcomings of the Peinado patent.

(b) The Rabin Patent Fails to Cure the Deficiencies of the Peinado Patent.

As outlined above, claim 1 of the present application recites a system for controlling use of digital content having usage rights associated therewith. The system comprises a server having digital content stored thereon, a client computer having a standard application program including a rendering engine, and a communications network coupled to the client and the server. The system recited in amended independent claim 1 also includes a client side security module, separate from the rendering engine, which is downloaded and included in the client computer. Further, claim 1 recites that the security module selectively intercepts a request to the rendering engine to render the digital content based upon the usage rights associated with the digital content and determines whether the requested digital content is protected content. The security module of claim 1 determines whether to allow a user

to perform a requested function on the protected digital content based upon the usage rights associated with the protected digital content. The security module then responds to the request to perform the requested function on the protected digital content based on the usage rights associated with the protected digital content and disengages from the rendering engine if the requested content is not protected content to preserve resources of the client computer.

The Rabin patent, in contrast, discusses methods and an apparatus for enabling owners and vendors of software products to protect property rights of their software by employing a vendor tag system. The Rabin patent describes a system that uses a tag server that produces a plurality of tags, one per instance of software, and the tags uniquely identify an instance of software with which the tag is associated. See col. 3, lines 47-53. A user device receives and installs an instance of software and receives a tag uniquely associated with that instance of software. See col. 3, lines 53-55. The user device includes a supervising program that detects attempts to use the instance of software and that verifies the authenticity of the tag associated with the instance of software before allowing use of the instance of software. See col. 3, lines 55-59. The supervising program on the user device verifies the authenticity of the tag and maintains or stores the tag in a tag table and maintains or stores the instance of software, if the tag is authentic. The supervising program rejects the instance of software if the tag associated with the software is not authentic. See col. 3, lines 59-65.

In the Final Office Action, the Examiner asserts that the Rabin patent discloses a security module that intercepts a request to the rendering engine, but the text cited by the Examiner in the Rabin patent instead discloses a system with a supervising program that regulates user requests to each instance of software. That is, the intercept is not selective and is not based upon usage rights associated with the digital content. For example, in column 11, lines 9-34, the Rabin patent discloses:

> The step of receiving the instance of software can include the step of obtaining the instance of software at the user device. And the step of receiving the tag at a user device can include the steps of securely obtaining the tag associated with the

> instance of software at the user device and determining if the tag associated with the instance of software is signed, and if so, verifying a signature on a hash function value in the tag and if the signature on the hash function value is verified, installing the software on the user device, and if the tag associated with the instance of software is not signed, installing the instance of software on the user device. The step of detecting an attempt to use the instance of the software on the user device can include the steps of invoking a supervising program on the user device to intercept a user request for use of the instance of software. The step of determining if the attempt to use the instance of the software is allowable can also include the steps of determining if a call-up procedure is needed based on a call-up policy and if so performing a call-up procedure to verify the authenticity and to determine the usage supervision policy of the tag associated with the instance of software. Also included are the steps of updating tag information in the user device based upon an outcome of the call-up procedure an examining status information associated with the tag to determine if use of the instance of software associated with the tag is allowed.

See the Rabin patent at col. 11, lines 9-34 (emphasis added).

As outlined above, the Rabin patent describes a method for supervising usage of software by creating an instance of software and creating a tag that is uniquely associated with the instance of software. The instance of software is then distributed, and the tag is securely distributed to a user device that receives the instance of software and the associated tag. When an attempt to access the instance of the software on the user device method is detected, the system determines if the attempt to use the instance of the software is allowable by determining a status of the tag that is associated with the instance of software to be used. See col. 10, lines 44-55. The Rabin patent supervises usage by distributing the software and the tag to a user device and later checking to make sure the status of the tag associated with that software is proper. The system of the Rabin patent appears to regulate all access to the software.

The present application, on the other hand, limits access to software only if the security module determines that the requested digital content is protected content. To effect this determination, the security module examines the usage rights associated with the digital content and selectively intercepts a request to the rendering engine to render the digital content. In the present application, this conditional checking and

selective intercept of requests may be employed to regulate access based on usage rules associated with the content. This is not the case in the Rabin patent. The regulation described in the Rabin patent is whether or not the user is authorized to use the software. That is, in the Rabin patent, the usage rights associated with the digital content are not the basis for selectively intercepting request. The system of the Rabin patent intercepts all requests and evaluates the software to make a determination as to whether the digital content is protected content. In the present application, access is regulated based upon whether or not the requested action would violate the usage rights associated with the content.

There is no disclosure in the Rabin patent of a security module that selectively intercepts a request to the rendering engine to render the digital content based on the usage rights associated with the digital content, nor of a security module that, if it determines that the requested digital content is protected content, further determining whether to allow a user to perform a requested function on the protected digital content based upon the usage rights associated with the protected digital content, and responding to the request to perform the requested function on the protected digital content based on the usage rights associated with the protected digital content. The system of the Rabin patent examines the status of the tag that is associated with each instance of software to be used, while the present application evaluates the usage rights associated with the content only if it determines that the requested content is protected content, as recited in claim 1, for example.

Additionally, amended independent claim 1 of the present application recites that the security module disengages from the rendering engine if the requested content is not protected content to preserve resources of the client computer. See paragraph [0066] of the present specification.

Neither the Rabin patent nor the Peinado patent disclose or suggest a security module with this feature. Instead, the Rabin patent describes supervising usage by distributing software and a tag to a user device and later checking to make sure the status of the tag associated with that software is proper. The system of the Rabin patent appears to regulate all access to the software and maintains regulation of the

software. That is, the tag checking is never disengaged from the rendering engine if the requested content is not protected content. As such, the system of the Rabin patent requires additional client computing resources to effect these checks.

The combination of the Rabin patent and the Peinado patent fails to disclose or suggest all the features recited in amended independent claim 1 of the present application. As such, Applicants respectfully submit that the combination of the Rabin patent and the Peinado patent fails to render claim 1 obvious under 35 U.S.C. § 103(a). Accordingly, Applicants respectfully submit that claim 1 of the present application is allowable over the combination of prior art as outlined above. Applicants respectfully request reconsideration and withdrawal of the rejection of claim 1 under 35 U.S.C. § 103(a).

2. The Combination of the Peinado Patent and the Rabin Patent Fails to Disclose or Suggest All the Features Recited in Dependent Claims 2-23, claims 26-34, and claims 36, 76, and 77.

Dependent claims 2-23, 26-34, claim 36, 76, and 77 depend upon amended independent claim 1, and thereby include all the limitations of independent claim 1, while reciting additional features of the present invention. As noted above, Applicants amended independent claims 1 and 37 to include limitations not disclosed or suggested by the combination of the Peinado patent and the Rabin patent. Accordingly, with the dependency of claims 2-23, 26-34, claim 36, 76, and 77 on amended independent claims 1, Applicants respectfully submit that the combination of references also fails to disclose or suggest all of the features and limitations of these dependent claims as well. As such, Applicant respectfully submits that the combination of references fails to render dependent claims 2-23, 26-34, claim 36, 76, and 77 obvious under 35 U.S.C. § 103(a) and that dependent claims 2-23, 26-34, claim 36, 76, and 77 are in proper condition for allowance. Applicant respectfully requests reconsideration of dependent claims 2-23, 26-34, claim 36, 76, and 77 and the withdrawal of the rejections under 35 U.S.C. § 103(a).

3. The Combination of the Peinado Patent and the Rabin Patent Fails to Disclose or Suggest All the Features Recited in Amended Independent Claim 37.

Independent claim 37 relates to a method for controlling use of digital content that has usage rights associated with the digital content. The method includes storing digital content on a server and a client requesting the digital content over a communications network. See, for example, Figs. 2 and 3, and the discussions that follow in at least paragraphs [0022, 0049-0052] and throughout the specification discussing distributor server 220. The client includes a standard application program with a rendering engine capable of being accessed to render content. See, for example, Figs. 2, 3, 7, 8, 10, and 11, and the discussions that follow in at least paragraphs [0022, 0049, 0051-0055, 0057, 0058, 0064-0072, 0078-0081, 0086-0088] and throughout the specification discussing client computer 230.

The method for controlling use of digital content also includes enforcing security conditions for accessing the rendering engine with a client side security module. The client side security module is separate from the rendering engine and is downloaded and included in the client computer. The security module is adapted to be attached to the standard application program for enforcing security conditions. See also, Figs. 2, 5, 6, 11, 13 and the discussions that follow in at least paragraphs [0022, 0049, 0051-0062, 0064-0067, 0078-082, 0086-0092, 0098-0105, 0108, 0111, 0114] and throughout the specification discussing security module 237. Enforcing security conditions includes the client side security module determining whether the requested digital content is protected content based upon the usage rights associated with the digital content and selectively intercepting a request to the rendering engine to render the protected digital content if the client side security module determines that the requested digital content is protected content. If the client side security module determines that the requested digital content is protected content, the client side security module determines whether to allow a user to perform a requested function on the protected digital content based on the usage rights associated with the digital content.

If the client side security module determines that the requested digital content is protected content, the client side security module responds to the request to allow a user to perform a requested function on the protected digital content based on the usage rights associated with the digital content. If the client side security module determines that the requested content is not protected content, the client side security module disengages from the rendering engine to preserve resources of the client computer. See Fig. 4, step 410 (step E) and paragraphs [0059-0061] for intercepting the request. See Figs. 2 and 4, regarding security module 237, UI module 234, and connection module 236 and paragraphs [0053-0061] for determining if the requested digital content is protected content and granting or denying the rendering request based on the usage rights associated with the digital content.

Independent claim 37 recites a method for controlling use of digital content that has usage rights associated with the digital content that is carried out by the system recited in independent claim 1. As such, claims 1 and 37 are related claims that recite a system and method, respectively, for controlling use of digital content that has usage rights associated with the digital content in accordance with the present invention.

As outlined above with regard to claim 1, the combination of the Peinado patent and the Rabin patent fails to disclose or suggest all the elements and limitations recited in independent claim 1 of the present application. Similarly, the combination of the Peinado patent and the Rabin patent also fails to disclose or suggest all the related steps and limitations of amended independent claim 37 as well. Therefore, Applicants respectfully submit that amended independent claim 37 is allowable over the combination of cited references for at least the reasons outlined above with regard to claim 1. Applicants respectfully request reconsideration and withdrawal of the rejection of claim 37 under 35 U.S.C. § 103(a).

4. The Combination of the Peinado Patent and the Rabin Patent Fails to Disclose or Suggest All the Features Recited in Dependent Claims 38-59, claims 62-70, and claims 72, 78, and 79.

Dependent claims 38-59, claims 62-70, and claims 72, 78, and 79 depend upon amended independent claim 37, and thereby include all the limitations of independent claim 37, while reciting additional features of the present invention. As noted above, Applicants amended independent claims 1 and 37 to include limitations not disclosed or suggested by the combination of the Peinado patent and the Rabin patent. Accordingly, with the dependency of claims 38-59, claims 62-70, and claims 72, 78, and 79 on amended independent claims 37, Applicants respectfully submit that the combination of references also fails to disclose or suggest all of the features and limitations of these dependent claims as well. As such, Applicant respectfully submits that the combination of references fails to render dependent claims 38-59, claims 62-70, and claims 72, 78, and 79 obvious under 35 U.S.C. § 103(a) and that dependent claims 38-59, claims 62-70, and claims 72, 78, and 79 are in proper condition for allowance. Applicant respectfully requests reconsideration of dependent claims 38-59, claims 62-70, and claims 72, 78, and 79 and the withdrawal of the rejections under 35 U.S.C. § 103(a).

D. Conclusion

In view of the above amendments and remarks, Applicants respectfully request that the Examiner reconsider this application and withdraw the rejections of record. Applicants respectfully request that the Examiner allow the pending claims and pass the present application to issue. If any issue remains after considering this response, Applicants invite the Examiner to call the undersigned to work out any such issue by telephone.

Except for issue fees payable under 37 C.F.R. § 1.18, the Commissioner is hereby authorized by this paper to charge any additional fees during the entire pendency of this application, including fees due under 37 C.F.R. §§ 1.16 and 1.17

which may be required, including any required extension of time fees, or to credit any overpayment to Deposit Account No. 19-2380. This paragraph is intended to be a CONSTRUCTIVE **PETITION FOR EXTENSION OF TIME** in accordance with 37 C.F.R. § 1.136(a)(3).

Respectfully submitted,

NIXON PEABODY, LLP

/Joseph A. Parisi, Reg. No. 53,435/
Joseph A. Parisi

NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, DC 20004
(202) 585-5000
(202) 585-8080 (Fax)